④

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-036559
(43)Date of publication of application : 07.02.1995

(51)Int.Cl. G06F 1/00
G06F 1/14
G06F 15/00

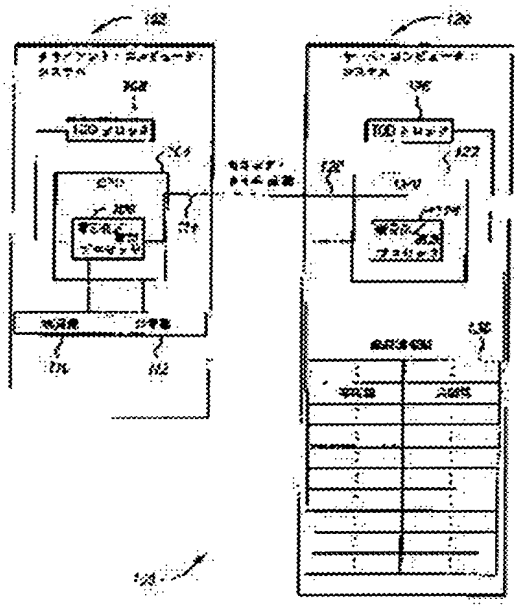
(21)Application number : 06-140369
(22)Date of filing : 22.06.1994

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : HARTMAN JR ROBERT C

(30)Priority
Priority number : 93 96132 Priority date : 22.07.1993 Priority country : US

(54) SECURE TIME KEEPING DEVICE AND SECURE TIME SERVER

(57)Abstract:
PURPOSE: To allow a client system to function without a reliable time value by allowing a server to ciphering a present time value from a TOD clock through the use of a private key corresponding to a requesting client to send the present time value through an open communication line.
CONSTITUTION: At the time of receiving a secure time request at a server I/O port 128, an electronic storage device 130 accesses the private and secret key for mutual reference based on an open clock. Reading a value from a server TOD clock 126, a ciphering/deciphering processor 124 ciphers the value through the use of the private key for mutual reference. A server system 120 prepares a responding transmission including ciphered time and date information, sends it back to the client system and writes it in a client TOD clock 108. The reliable time value of the client TOD clock is used for executing a time limit set to a media licence.



LEGAL STATUS

[Date of request for examination] 22.06.1994
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2628619

[Date of registration]	18.04.1997
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	18.04.2000

Japanese Patent Laid-open Publication No. HEI 7-36559 A

Publication date : February 7, 1995

Applicant : INTERNATL BUSINESS MACH CORP <IBM>

Title : SECURE TIME KEEPING DEVICE AND SECURE TIME SERVER

[0027] The client computer system 102 must periodically initiate a secure time transmission when it operates in a secure time request-receive network. Alternatively, when it operates in a secure time broadcast network, the server periodically initiates the transmission without requiring a request from the client. In the request-receive network, the client computer processor 202 sends a secure time request to the server 120 to initiate a secure time transmission. This request is generated by the CPU 104 and includes current values for various components of the secure timekeeping device 214. In other words, it includes values for the TOD clock 108, the authenticated time indicator 218, the precision maintenance register 220, the correction adjustment register 222, and the public key 112. According to the preferred embodiment, this information is collected simply by GET CURRENT TIME command and includes MAC in order to avoid the recording-playback problem. In any case, this information is encrypted by the encryption/decryption processor 106 using a private key of the client, which will be included in the transmission along with a client's public key, and is

transferred to the server system through the I/O port 114. As shown in Fig. 4, the server system subsequently calculates a new precision maintenance value and a new correction adjustment value, generates a new client TOD clock value, encrypts the information using the private key corresponding to the client's public key (the same holds for the MAC according to the preferred embodiment), and returns the encrypted information to the client computer system 102. Upon receiving the information, the encryption/decryption processor 106 uses the private key 110 to decrypt these new values, namely, the TOD clock value, the precision maintenance value and the correction adjustment value. According to the preferred embodiment, the MAC is also decrypted and used when the server response is checked against the client request. Subsequently, the CPU 104 stores the new TOD clock value in the TOD clock 108, the new precision maintenance value in the precision maintenance register, and the new correction adjustment value in the correction adjustment register 220 to configure various other components of the secure timekeeping device 214. Finally, the authenticated time indicator 218 is set to TRUE to indicate that the encrypted time and date value have been successfully processed and that an authenticated reliable TOD clock value is currently in use.

[0028] In the secure time broadcast network, the client operation is the same as that described above, except that there is no client request raised. Instead, the server periodically generates a secure time broadcast that is encrypted by a client's private key

and identified by matching it with a client's public key. Alternatively, the server sends a secure time broadcast simultaneously to all clients after sending an encrypted master key to the all clients, while this broadcast is decrypted at the clients using the time master key that has been delivered prior to the broadcast. The server does not have sufficient data necessary to produce a new precision maintenance value and a correction adjustment value because these broadcasts occur without request being made for them. In other words, information for them is not incorporated in the operation under this mode. Upon receiving the broadcast secure time transmission, a new TOD clock value is decrypted and provided to the TOD clock 108 as described above, while the authenticated time indicator 218 is set TRUE.

[0029] In the preferred embodiment, if message verification is necessary, the client initiate a broadcast mode by first performing a transmission that includes a first MAC. When the server subsequently broadcasts a secure time transmission to the client, it includes the first MAC in the transmission. The client acknowledges that it has received the transmission by sending a new MAC that will be used when the server performs the next secure time transmission. This process is repeated in each subsequent broadcast. Also in this broadcast mode operation involving MAC, values for the client TOD clock, an authenticated time indicator, a precision maintenance register, and a correction adjustment register can be incorporated in the client acknowledgement. This

helps to alleviate the above mentioned disadvantage to some extent, and to enable the server to provide an updated precision maintenance value and correction adjustment value in the next broadcast. These values are not accurate compared with those in the request-receive mode. This is due to a fact that the next broadcast takes place long after the acknowledgement that constitutes the basis for these values. However, this problem itself can be addressed by increasing the frequency of broadcasts within the bandwidth limits of the client.

[0030] Fig. 3 represents an additional mechanism provided in the client computer system 102 to monitor the integrity of the power supply. A power integrity monitor 302 is added to the secure timekeeping device 214 in the package 216 that is physically secure. The power integrity monitor 302 is connected to other components for secure timekeeping including the CPU 104, the TOD clock 108, the authenticated time indicator 218, the precision maintenance register 220, and the correction adjustment register 222, via an electronic circuit for monitoring (indicated by the dashed line). During its operation, the power integrity monitor 302 continually monitors the voltage level for the above mentioned components against predefined normal ranges representing operation limits of the electronic elements used in the client computer system. If a supplied regular voltage or a voltage for the backup purpose reduces to fall outside a range that is required for maintaining a stable and correct operation of the secure timekeeping device component,

then the power integrity monitor 302 sets the value of the authenticated time indicator 218 to FALSE to indicate that the TOD clock 108 is no longer reliable.

[0031] It should be noted that many variations are possible for the power integrity monitor 302. For example, the power integrity monitor 302 can be configured so that it monitors the voltage of the TOD clock 108 only, or it only monitors any one of other components rather than monitoring all the components in the secure timekeeping device. In another example, the power line to the secure timekeeping device 214 can be designed so that a single power input path is provided. In this case, the power integrity monitor 302 can directly monitor the power input path instead of monitoring individual components. Specific electronic elements and low level elements selected for performing the power integrity monitoring function in 302 ultimately become a basis for the design selection. This issue is covered by many known literatures, and therefore not explained here.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－36559

(43)公開日　平成７年(1995)２月７日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	1/00	３７０　Ｅ				
	1/14					
	15/00	３３０　Ａ	7459－5Ｌ			
			7165－5Ｂ	Ｇ０６Ｆ	1/ 04	３５０

審査請求　有　請求項の数30　ＯＬ　（全 17 頁）

(21)出願番号　特願平6－140369

(22)出願日　平成６年(1994)６月22日

(31)優先権主張番号　９６１３２

(32)優先日　1993年７月22日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　ロバート・チャールズ・ハルトマン、ジュニア
アメリカ合衆国94062－0717　カリフォルニア州、ウッドサイド、ピー・オー・ボックス620717（番地なし）

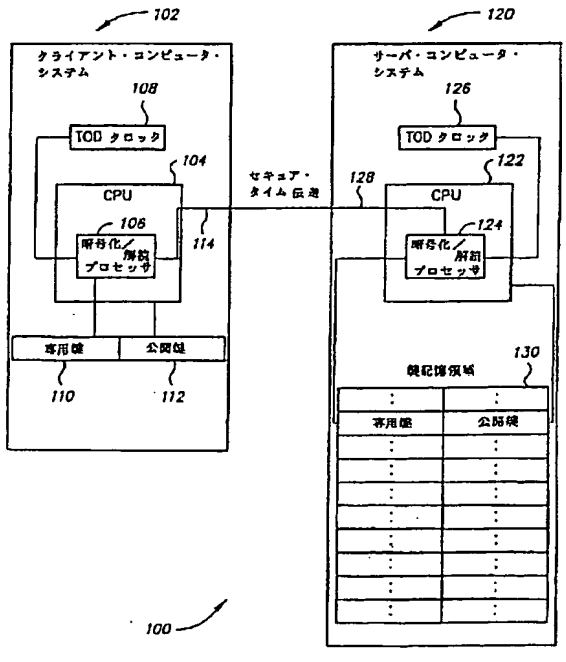
(74)代理人　弁理士　合田　潔　（外２名）

(54)【発明の名称】　セキュア・タイムキーピング装置

(57)【要約】

【目的】　クライアント・サーバベースのセキュア・タイムキーピング機構を備えたコンピュータ・システムを提供する。

【構成】　物理的に信頼できる環境に設置されたセキュア・タイム・サーバが、高精度の日時（ＴＯＤ）クロックを有し、クライアント／サーバ・ネットワークにおけるクライアントに対応する公開鍵／専用鍵の対のテーブルを格納した鍵記憶領域を備える。サーバは、選択されたクライアントに対応する専用鍵を用いてそのＴＯＤクロックから現在の時刻値を暗号化する。暗号化された時刻値はオープンな通信チャネルを介してそのクライアントへ送られる。各クライアントは、不正に対向できる１つのＶＬＳＩチップの安全な区域内に収容された固有のセキュア・タイムキーピング装置を有する。



セキュア・タイム・クライアント／サーバ・システム

1

【特許請求の範囲】

【請求項１】物理的に安全確保されたパッケージ内に設置された中央演算処理装置と電子記憶装置とを含むコンピュータ・システムにおいて用いるセキュア（安全確保された）・タイムキーピング装置であって、

時刻伝送及び日付伝送を暗号化しかつ解読するために専用鍵を識別するときに用いる公開鍵を保有する公開鍵レジスタと、

前記専用鍵を保有する専用鍵レジスタと、

前記専用鍵を用いて暗号化された時刻及び日付の情報を受信する入力と、

前記専用鍵を用いて受信された時刻及び日付の情報を解読するデータ解読手段と、

前記解読された時刻及び日付の情報を受信するための入力及び暗号化されていない時刻及び日付の情報を与えるための出力を備え、時刻クロックと日付カレンダーとを含む日時（time-of-day：ＴＯＤ）クロックとを有するセキュア・タイムキーピング装置。

【請求項２】前記ＴＯＤクロックが前記中央演算処理装置と同じ物理的に安全確保されたパッケージ内に設置される請求項１に記載のセキュア・タイムキーピング装置。

【請求項３】前記公開鍵が、前記コンピュータ・システムのシステム・シリアル番号に対応する請求項１に記載のセキュア・タイムキーピング装置。

【請求項４】前記公開鍵が前記コンピュータ・システムに固有のものでありかつ物理的に安全確保されたパッケージの外部からアクセス可能である請求項１に記載のセキュア・タイムキーピング装置。

【請求項５】前記専用鍵が前記コンピュータ・システムに固有のものでありかつ物理的に安全確保されたパッケージの外部からアクセス不能である請求項１に記載のセキュア・タイムキーピング装置。

【請求項６】前記専用鍵を用いて暗号化された現在の時刻及び日付の情報のいずれかを時刻サーバに対して要求するセキュア・タイム（安全確保された時刻）要求手段を有する請求項１に記載のセキュア・タイムキーピング装置。

【請求項７】前記セキュア・タイム要求手段により開始された要求が前記ＴＯＤクロックの現在値を含む請求項６に記載のセキュア・タイムキーピング装置。

【請求項８】時刻及び日付のいずれかの更正値を受信しかつ該更正値を前記ＴＯＤクロックに適用するクライアント・クロック更正手段を有する請求項１に記載のセキュア・タイムキーピング装置。

【請求項９】前記更正値が専用鍵を用いて暗号化される請求項８に記載のセキュア・タイムキーピング装置。

【請求項１０】物理的に安全確保されたパッケージ内に設置された中央演算処理装置と電子記憶装置とを含むコンピュータ・システムにおいて用いるセキュア（安全確保された）・タイムキーピング装置であって、

2

時刻クロックと日付カレンダーとを含む日時（time-of-day：ＴＯＤ）クロックと、

前記ＴＯＤクロックが認証された時刻及び日付を有するか否かを示す値を記憶する認証時刻インジケータと、

前記ＴＯＤクロックが正確であると見なされる持続時間を示す値を記憶する精度持続レジスタと、

時刻、日付、及び精度持続時間のいずれかの値を受信する入力と、

前記ＴＯＤクロックからの暗号化されていない時刻及び日付の値と前記認証時刻インジケータからの値を与える出力とを有するセキュア・タイムキーピング装置。

【請求項１１】前記精度持続レジスタが時刻の値を格納し、前記認証時刻インジケータが、暗号化された値を用いて前記ＴＯＤクロックをセットしたことと、暗号化された値を用いて前記精度持続レジスタをセットしたことと、該精度持続レジスタが該ＴＯＤクロックの値より時間的に大きい（遅い）値を格納していることとを満たすことに応答してＴＲＵＥにセットされる請求項１０に記載のセキュア・タイムキーピング装置。

【請求項１２】前記認証時刻インジケータが、システムの初期化、動作電圧低下状態、ＴＯＤクロックを暗号化されていない値を用いてセットしたこと、及び前記精度持続レジスタが該ＴＯＤクロックの値よりも時間的に小さい（早い）値を格納していることのいずれかに対してＦＡＬＳＥにセットされる請求項１１に記載のセキュア・タイムキーピング装置。

【請求項１３】受信された時刻、日付、及び精度持続の値に基づいてＴＯＤクロックの値及び精度持続レジスタの値をセットし、

受信された時刻、日付、及び精度持続の値が暗号化されていない場合に前記認証時刻インジケータをＦＡＬＳＥにセットし、受信された時刻、日付、及び精度持続の値が暗号化されておりかつ前記精度持続レジスタにセットされた値が前記ＴＯＤクロックにセットされた値よりも時間的に大きい場合に該認証時刻インジケータをＴＲＵＥにセットする時刻装置設定手段を有する請求項１０に記載のセキュア・タイムキーピング装置。

【請求項１４】前記セキュア・タイムキーピング装置が、ＴＯＤクロックが更正調整を受信すべき時間間隔を示す値を記憶する更正調整レジスタを有し、

前記入力が、更正調整の値を受信するための手段を有し、

前記時刻設定手段が、前記受信された更正調整の値に基づいて前記更正調整レジスタをセットする手段を有する請求項１３に記載のセキュア・タイムキーピング装置。

【請求項１５】操作により前記ＴＯＤクロック及び前記更正調整レジスタに接続されかつ該ＴＯＤクロックが該更正調整レジスタの値に増分される毎に該ＴＯＤクロックに対する更正調整を行うＴＯＤクロック更正器を有す

る請求項１４に記載のセキュア・タイムキーピング装置。

【請求項１６】前記更正調整レジスタの値が、増分、飛び、及び非調整のいずれかを示し、

更正調整の値が増分を示す場合は、前記ＴＯＤクロックに適用される更正調整が１つの加算的増分であり、

更正調整の値が飛びを示す場合は、前記ＴＯＤクロックに適用される更正調整が１つの飛びであり、

更正調整の値が非調整を示す場合は、前記ＴＯＤクロックに適用される更正調整が増分ゼロである請求項１５に記載のセキュア・タイムキーピング装置。

【請求項１７】正の更正調整値が増分を示し、負の更正調整値が飛びを示し、及びゼロの更正調整値が非調整を示す請求項１６に記載のタイム・キーピング装置。

【請求項１８】前記ＴＯＤクロック、前記認証時刻インジケータ、前記精度持続レジスタ、及び前記更正調整レジスタの暗号化されていない値を読取る時刻装置読取り手段を有する請求項１６に記載のセキュア・タイムキーピング装置。

【請求項１９】前記更正調整レジスタの値が前記ＴＯＤクロックを最後にセットしてから該ＴＯＤ内に積算されたドリフト量の関数であり、前記精度持続レジスタの値が該ドリフト量と該ＴＯＤクロックの先の設定に対応する予め測定されたドリフト量との比較に基づく請求項１８に記載のセキュア・タイムキーピング装置。

【請求項２０】現在時刻、日付、及び精度持続の値のいずれかを時刻サーバから要求するセキュア・タイム要求手段を有し、

前記セキュア・タイム要求手段により開始された要求が、前記ＴＯＤクロックの現在値、前記精度持続レジスタの現在値、前記更正調整レジスタの現在値、及び認証時刻インジケータの現在値のいずれかを含む請求項１３に記載のセキュア・タイムキーピング装置。

【請求項２１】時刻クロックと日付カレンダーを含むサーバ日時（time-of-day：ＴＯＤ）クロックを有するコンピュータ・ネットワークにおけるセキュア（安全確保された）・タイム・サーバであって、

公開鍵を含むセキュア・タイム要求を受信する入力と、

前記公開鍵に対応する専用鍵を識別するプロセッサ手段と、

前記専用鍵を用いて前記ＴＯＤクロックからの時刻及び日付の情報を暗号化するデータ暗号化手段と、

前記セキュア・タイム要求を行った者に対して前記暗号化された時刻及び日付の情報を送る出力とを有するセキュア・タイム・サーバ。

【請求項２２】前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び更正履歴の情報、並びに前回のクライアント・クロック更正計算から積算された更正履歴のいずれかに基づいて該クライアント・クロック更正値を計算する更正調整手段を有する請求項

２１に記載のセキュア・タイム・サーバ。

【請求項２３】前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び安定度履歴の情報、並びに前回のクライアント・クロックの安定度計算から積算された安定度履歴のいずれかに基づいて該クライアント・クロックの安定度値を計算するクライアント安定度監視手段を有する請求項２１に記載のセキュア・タイム・サーバ。

【請求項２４】前記クライアント・クロック更正値が、さらに、前記クライアント・クロックの最後の設定以降該クライアント・クロックに積算されたドリフト量から計算される請求項２２に記載のセキュア・タイム・サーバ。

【請求項２５】前記更正値が、前記専用鍵を用いて暗号化される請求項２２に記載のセキュア・タイム・サーバ

【請求項２６】時刻クロックと日付カレンダーを含むサーバ日時（time-of-day：ＴＯＤ）クロックを有するコンピュータ・ネットワークにおけるセキュア（安全確保された）・タイム・サーバであって、

セキュア・タイム伝送を行うために公開鍵及び専用鍵を識別するプロセッサ手段と、

前記専用鍵を用いて前記ＴＯＤクロックからの時刻及び日付の情報を暗号化するデータ暗号化手段と、

前記暗号化された時刻及び日付の情報をブロードキャスト（同報通信）する出力とを有するセキュア・タイム・サーバ。

【請求項２７】前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び更正履歴の情報、並びに前回のクライアント・クロック更正計算から積算された更正履歴のいずれかに基づいて該クライアント・クロック更正値を計算する更正調整手段を有する請求項２６に記載のセキュア・タイム・サーバ。

【請求項２８】前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び安定度履歴の情報、並びに前回のクライアント・クロックの安定度計算から積算された安定度履歴のいずれかに基づいて該クライアント・クロックの安定度値を計算するクライアント安定度監視手段を有する請求項２６に記載のセキュア・タイム・サーバ。

【請求項２９】前記クライアント・クロック更正値が、さらに、前記クライアント・クロックの最後の設定以降該クライアント・クロックに積算されたドリフト量から計算される請求項２７に記載のセキュア・タイム・サーバ。

【請求項３０】前記更正値が、前記専用鍵を用いて暗号化される請求項２６に記載のセキュア・タイム・サーバ

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コンピュータのデータのセキュリティ（security）に関し、より詳細にはクラ

5

イアント・サーバ型コンピュータ・ネットワークに使用するセキュリティの確保されたセキュア・タイムキーピング（secure timekeeping）装置に関する。

【０００２】

【従来の技術】コンピュータ・システムにおけるメディア（すなわちデータ）のセキュリティは、従来、多重レベルで実現されている。第１のセキュリティ・レベルは、データへのアクセスを完全に拒否することを含む。アクセス・レベルのセキュリティを実現するために、パスワード保護、論理パーティション、及びデータ暗号化を含む多くの方法が存在する。暗号化の方法においては、多数の錠と鍵のアーキテクチャが開発されてきた。このようなアーキテクチャの１つが米国特許第９２８８５０号に開示されており、ここに参照する。上記特許によるアクセス・レベルのセキュリティは、ディジタル・メディアの使用を、メディアの中央処理機構（Media Clearinghouse：サーバ）によって与えられた適切な許諾特権を有するクライアント・ユーザに限定することを目的としている。元のディジタル・メディアとしては、ファイルまたはデータ・オブジェクトに含まれるプログラム・オブジェクト・コード、プログラム・ソース・コード、イメージ、音声、ビデオ、文書または他の形式の情報等があるが、これらは、内容作成者またはオーナーの代わりにメディアの中央処理機構によってメディア・マスター鍵（Media Master Key）で暗号化される。次に、メディア・マスター鍵は、許可されたクライアント・システムのそれぞれについての固有の専用鍵でさらに暗号化される。その後、暗号化されたメディア及び暗号化されたメディア・マスター鍵が、オープンで安全確保されていないチャネルを介して広範囲に分配される。

【０００３】別のメディア・セキュリティとしては、一旦アクセスが許可されると適用されるもので、時刻に基づいてアクセスを制限するものがある。クライアント／サーバ型ネットワークにおいては、時刻ベースの制限自体が、サーバによりアクセスを許可された時間帯と現在時刻との比較を行うものである。現在時刻は、通常、クライアントのコンピュータ・システムの日時（time of day：ＴＯＤ）クロックに記憶された時刻である。しかしながら、この比較と基本的に時刻ベースによる制限は、アクセス機構に対してアクセス時間帯が依然としてアクティブであると誤って認識させるようシステム・クロックを進めたり遅らせたり簡単にセットできる侵入者、倫理観に欠ける管理者、又は精通したユーザによって容易に無効にされてしまいがちである。さらに、たとえクライアントのＴＯＤクロックが侵害を受けにくいものであっても、オーバタイムによりその値が現在時刻からずれてしまうドリフトや不安定さといった不正確さを常に含みがちである。クロックのドリフトは、一定の度合いで時間を遅らせたり進めさせたりする予測可能な定常的な不正確さである。クロックの不安定さは、クロックのドリフト成分を変化させるような予測不能な不正確さである。不安定さを引き起こす要因としては、気温、湿度、電源電圧などが含まれる。最後に、前述の問題点よりもさらに悪い点は、電源遮断ような致命的な事故の場合、クライアントのＴＯＤ値が実際の現在時刻から急激にずれることである。

6

【０００４】従来の技術において、信頼性のある又は安全確保された時刻（セキュア・タイム：secure time）のソースを提供する課題は、サーバ・コンピュータ・システムから暗号化されたタイムスタンプを定期的に発生することによってこれまでは解決されてきた。１つの手法では、タイムスタンプがクライアントに送られ、そこで解読され、アクセスを制限するための基本として用いられる。この手法は、信頼性のある不連続な時刻値を与えることに限界があるという欠点を有する。すなわちこの手法は、クロック自身は信頼性があるので、クライアントＴＯＤクロックをセットし維持する問題に対処するものではない。第２の手法では、クライアントに電子文書を分配する前に、暗号化されたタイムスタンプがサーバによってその電子文書に与えられる。クライアント側において、タイムスタンプはその文書にアクセスするための基本として用いられる。しかしながら、前述の手法と同様にこのシステムは、安全確保されていない環境で安全性のあるＴＯＤクロックを提供することよりも、一定数の信用できるタイムスタンプを与えることの方に限界がある。

【０００５】セキュア・タイムを提供する第３の従来の手法は、サーバよりもむしろクライアントに注目したものである。クライアントのＴＯＤ機構は、最初は適当な時刻を用いてセットされる。次に、信頼できる監視者がこのセット時刻を検証することにより、この時刻を信頼できる時刻（trusted time）とする。各セットの間の正確さを維持するために、多数のクロックが用いられ、信頼できる時刻を得るためにそれらの値を平均化する。この方法は個々のタイムスタンプ及びドリフトや不安定の問題に対処しようとしたものであるが、そのセット自体に重大な欠点がある。第１に監視者は信頼できる時刻を確定しなければならないので、かなり小さなシステム以外では、すなわちネットワークのごく一部以外では実用的でない。第２に、検証プロセスは人間による介入を必要とするので、人間により通常被る全ての故障モードすなわちエラー、怠慢、ごまかしなどを受けやすい。第３に、正確さを維持するために多数のクロックを使用することは、高価でありかつ一貫性がない。多くの場合、平均値でさえ実際の時間からすぐにはずれてしまうであろう。

【０００６】最後の従来技術の方法は、クライアント及びサーバの双方に対して提供されるもので、前述したシステムの幾つかの欠点を解消するために開発された。この方法において、サーバは、秘密鍵、時刻値、及び認証

7

装置ＩＤを用いる暗号化された認証コードを作成する。次にサーバは、認証装置ＩＤ、暗号化認証コード、及びクライアントからのランダム数字に沿って、要求しているクライアント・コンピュータへ時刻を送る。この時刻を受け取ると、クライアントは暗号化認証コードとランダム数字をチェックし、時刻値のセキュリティを検証する。電源遮断により生ずる故障に対して保護するために、クライアントは、有効な暗号化認証コードとランダム数字をサーバが受取るまでは立上げを避ける機構を有する。

【０００７】

【発明が解決しようとする課題】この方法は、前述の問題点を改善しているけれども、ある欠点も負っており問題点も残っている。第１に、この方法は信頼できる時刻が得られなければクライアント・システムが動作しないため、クライアント・システムは信頼できる時刻へのアクセスを必要としないタスクでさえも用いることができない。第２に、クライアント・クロックにおけるドリフト及び不安定の問題に対処していない。従って、クライアントのＴＯＤクロックが不正確なためにすぐに信頼性が無くなることになる。

【０００８】以上のように、クライアント／サーバ型ネットワークに用いるセキュア・タイムキーピング装置の必要性に対して適切な対応がなされていない。本発明の目的は、クライアントのＴＯＤクロックをセットするためにサーバが発生した信頼できる時刻値を提供することにより、クライアント・システムは信頼できる時刻値がなくても機能し、さらに一旦信頼できる時刻値を与えると、クライアント・クロックの正確さを維持するような装置を提供することである。

【０００９】

【課題を解決するための手段】本発明によれば、クライアント／サーバベースの安全確保されたタイムキーピング・コンピュータ・システムを提供する。セキュア・タイム・サーバ・コンピュータ・システムは、物理的に信頼性のある環境に設置されており、クライアント／サーバ型ネットワークにおけるクライアントに対応する公開／専用鍵対のテーブルを含む鍵記憶エリアとともに、高精度の時刻（ＴＯＤ）クロックを有する。クライアントベースの要求に応答して、またはインターバル・ブロードキャスト（interval-broadcasting）方法の一部分として、サーバは要求しているクライアントまたは選択されたクライアントに対応する専用鍵を用いてそのＴＯＤクロックから現在時刻値を暗号化する。次に、暗号化された時刻値はオープンな通信チャネルを介してクライアントへ送られる。

【００１０】ネットワークの各クライアントは、公開／専用鍵の対、中央演算処理装置（ＣＰＵ）及び解読機構を含む自分自身のセキュア・タイムキーピング装置を備えており、そのすべてが、１つの不正対応ＶＬＳＩチップの安全領域内に格納されている。セキュア・タイムの伝送を受け取ると、クライアントはその専用鍵の自分自身のコピーを用いて時刻値を解読し、次に解読された時刻値をそのＴＯＤクロックにロードする。

8

【００１１】鍵の対、ＣＰＵ、及び解読機構に加えて、各クライアントにおける不正対応ＶＬＳＩチップ（セキュア・タイムキーピング装置）は認証時刻インジケータを有する。このインジケータは、ＴＯＤクロックが信頼できる時刻を有することを示す場合はＴＲＵＥにセットされ、ＴＯＤクロックの現時刻が信頼できないことを示す場合はＦＡＬＳＥにセットされる。認証時刻インジケータは、クライアント・システムがパワーオンされるとき、または電圧低下状態が検出されるとき、ＦＡＬＳＥに初期化される。クライアント・プログラムは、認証時刻インジケータを読取り専用ベースで利用することができる。セキュア・タイムを必要とするプログラムは、実行前に認証時刻インジケータを検査しなければならない。一方、セキュア・タイムを必要としないプログラムは、無関係に実行することができる。よって、たとえ信頼できる時刻値が得られなくても、有用な処理タスクは依然としてクライアント・コンピュータ・システム上で実行される。

【００１２】一旦、クライアントＴＯＤクロックの信頼できる時刻値がセットされた後にその正確さを継続的に維持するために、セキュア・タイムキーピング装置はさらに、更正機構とクロック安定性監視機構とを備えている。更正調整レジスタ、精度持続レジスタ、及びクロック更正器がクライアントの不正対応ＶＬＳＩチップ内に設けられる。サーバ・システム内では、ＣＰＵはクライアント・クロックの更正調整値及びクライアント・クロックの安定値を計算する機能を備えている。さらに別のサーバ記憶装置が、様々なクライアント・クロックに対してその更正履歴と安定性履歴とを保持するために設けられている。

【００１３】クライアントがセキュア・タイム値を要求するとき、その要求の中には、認証時刻インジケータ、そのＴＯＤクロック、その更正調整レジスタ及びその精度持続レジスタの現在値が含まれる。要求を受け取ると、サーバはまず認証時刻インジケータの値がＴＲＵＥかどうかを判断する。もしＴＲＵＥであれば、サーバは受け取ったＴＯＤクロック値とサーバのＴＯＤクロックの現在値との差（クライアント・クロックのドリフト）を用いて、クライアント・クロックの新しい更正調整値を計算する。次に、サーバは、そのクライアントについて記憶された安定度データに対するクライアント・クロックのドリフトと受け取ったクライアント精度持続値とを比較し、新しい精度持続値を計算する。最後に、サーバは、クライアント・クロックの新しい更正値と精度持続値を現サーバのＴＯＤクロック値とともに暗号化し、クライアントへの応答を伝送する。

9

【００１４】サーバからの応答を受け取ると、クライアントはその専用鍵を用いて更正調整値、精度持続値及びＴＯＤクロック値を解読する。更正調整値と精度持続値は、それぞれのレジスタに記憶される。ＴＯＤクロックは、そのＴＯＤクロック値でセットされ、認証時刻インジケータはＴＲＵＥにセットされる。クライアントのＴＯＤクロックが進行するにともない、更正機構は更正調整レジスタの値に従って定期的に時刻を調整する。一方、クライアントＣＰＵは、精度持続レジスタに対するＴＯＤクロックの進行を追跡する。ＴＯＤクロックが精度持続レジスタによって指示された時刻に到達すると、認証時刻インジケータはＦＡＬＳＥにセットされ、信頼できる時刻を必要とする処理をそれ以上行わないようにする。

【００１５】

【実施例】図１に、本発明によるクライアント／サーバベースの安全確保されたタイムキーピング・システムの基本的な機能を説明した機能図を示す。コンピュータ・ネットワーク１００は、クライアント・コンピュータ・システム１０２とサーバ・コンピュータ・システム１２０とを有する。クライアント・コンピュータ・システム１０２は、データ暗号化／解読プロセッサ１０６を組込んだクライアント中央処理装置（ＣＰＵ）１０４、時刻（ＴＯＤ）クロック１０８、専用鍵レジスタ１１０、公開鍵レジスタ１１２、及びセキュア・タイムのデータ伝送を要求し受け取る入出力（Ｉ／Ｏ）ポート１１４をさらに有する。サーバ・コンピュータ・システム１２０は、データ暗号化／解読プロセッサ１２４を組込んだサーバＣＰＵ１２２、ＴＯＤクロック１２６、Ｉ／Ｏポート１２８、及び電子記憶装置１３０をさらに有する。クライアント及びサーバの双方のＴＯＤクロック１０８及び１２６は、時刻クロックと日付カレンダーを有する。クライアントＴＯＤクロック１０８は、クライアント・コンピュータ・システムの製品寿命の間には０に戻らないことを保証できるだけの十分なビット数を有することが好ましい。サーバＴＯＤクロック１２６は、好適にはグリニッジ標準時（ＧＭＴ）に定期的に同期させられ、そしてＧＭＴもしくは協定世界時（Coordinated Universal Time）による時刻値またはＧＭＴからずれたいずれかの地域における時刻値を報告する。公開鍵レジスタ１１２に記憶されたクライアントの公開鍵の値は、クライアント・システムを独自に識別する任意の値である。この値は、クライアント・システムのシステム・シリアル番号であることが好ましい。専用鍵レジスタ１１０に記憶されたクライアントの専用鍵は、サーバの電子記憶装置１３０に格納された同様の専用鍵と対応している。どちらの専用鍵もユーザに利用できるようには作成されていない。公開／専用鍵システム、そのアーキテクチャ及び利用の詳細については本発明の要旨ではないが、前述の米国特許第９２８８５０号に開示されている。公開されている文献に記載された鍵ベースの安全確保アーキテクチャは、本発明を用いて容易に置換えることができる。

10

【００１６】動作中に、サーバ・コンピュータ・システム１２０は、１又は複数のクライアント・コンピュータ・システム１０２によって用いられるセキュア・タイム情報を提供する。本発明の一実施例では、セキュア・タイムの伝送は、クライアント・コンピュータ・システム１０２により出された要求で開始される。この要求は公開鍵レジスタ１１２の値を含み、そしてＩ／Ｏポートを経て、オープンで安全確保されていない通信チャネルを介してサーバ１２０へ送られる。公開鍵の値は、クライアント・コンピュータ・システムの製造業者のシリアル番号、またはクライアント・コンピュータ・システムが利用できる他の任意の固有の識別子である。ユーザが、その後に続くサーバの伝送を妨害したり、公開鍵の値を記録したり、後にクライアントへ再生したり（それによって、信頼できる時刻を提供するシステムの機能が損なわれる）できないように、メッセージ認証コード（ＭＡＣ）も、クライアントの要求伝送に含まれる。このＭＡＣは、個々のセキュア・タイム要求を識別するためにクライアントにより作成される固有のストリングである。これは、伝送に先立ちクライアントによって暗号化される。引き続いてサーバが安全確保された時刻値を伝送するとき、そのＭＡＣはクライアントへ返送される。クライアントは、要求のために作成したＭＡＣと返送されたＭＡＣを照合することにより、サーバによる伝送が、先に行ったいずれかの要求に対する応答ではなく本当に今現在行っている要求に対する応答であることを確認する。ＭＡＣの利用については、公知の暗号文献に詳細に説明されているので本明細書では繰返して述べない。前述の識別基準に適合するいずれの利用可能なＭＡＣ方法であっても、ＣＰＵ１０４におけるサポート機能と関連する１又は複数の別のレジスタを用いることにより、本発明とともに実施することができる。

【００１７】サーバＩ／Ｏポート１２８においてセキュア・タイム要求を受取ると、電子記憶装置１３０は、公開鍵に基づいて相互参照の専用秘密鍵へアクセスされる。サーバＴＯＤクロック１２６から値が読取られ、暗号化／解読プロセッサ１２４が相互参照の専用鍵を用いてその値を暗号化する。次にサーバ・システム１２０は、暗号化された時刻と日付情報を含む応答伝送を作成し、Ｉ／Ｏポート１２８を介してその伝送をクライアント・システム１０２へ送り返す。

【００１８】クライアント・システム１０２においてセキュア・タイムの応答が受取られると、専用鍵レジスタ１１０から専用鍵のクライアントによる複写が抽出され、暗号化されていない時刻及び日付情報を発生するために暗号化／解読プロセッサ１０６により用いられる。そしてそれらの情報はクライアントＴＯＤクロック１０

８へ書込まれる。クライアントＴＯＤクロック１０８の信頼できる時刻値は、引き続いてメディア・ライセンス（媒体許可）に設定された時間制限を実効化するために用いられる。従って、例えばデジタル・ビデオ伝送やソフトウェア・パッケージの試用複写とともに受信された電子的ライセンスによりそのライセンスが時刻Ｘに切れるべきであることが示された場合、そのビデオの映写やソフトウェアの実行を行う前にクライアント・システムの許可ソフトウェアによりＴＯＤクロックの検査が行われる。もしＴＯＤクロック値が時刻Ｘ以前の時刻であれば、許可ソフトウェアは、映写や実行を開始することを許可する。もしＴＯＤクロック値が時刻Ｘを過ぎていれば、許可ソフトウェアは、許可時間の満了に基づき映写や実行を禁止する。クライアントの視点からみると、クライアント・システム（消費者）が人間の介入を必要とすることなく高精度のＴＯＤクロックを与えられると云う別の利点が明らかである。さらに、クライアントＴＯＤクロックは、所望のフォームで表示することが可能である。そしてまた、ユーザにとっての利点は、サーバが、日光節約時間（daylight saving time）等の法令により定められた時刻変更に関しても任意に更新を行うことができることである。これにより、消費者はこれらの頻度の少ない事象を覚えておく必要がなくなる。

【００１９】図２は、本発明によるセキュア・タイムキーピング機構を有するクライアント・コンピュータ・システムの構造と相互関係を詳細に示した機能図である。クライアント・コンピュータ・システムは１０２で示されている。このシステムは、クライアント・コンピュータ・プロセッサ２０２、表示画面２０４、入力装置２０６、外部記憶装置２０８、及びＩ／Ｏポート１１４を含む。入力装置２０６は、キーボード、ジョイスティック又は他のいずれかのオペレーターマシン間通信装置である。外部記憶装置２０８としては、ランダム・アクセス・メモリ、ディスク記憶装置、テープ記憶装置等がある。クライアント・コンピュータ・プロセッサ２０２は、セキュア・タイムキーピング機構２１４を含む。セキュア・タイムキーピング機構は、その全体が物理的に安全確保された電子パッケージ２１６に格納されている。セキュア・パッケージ２１６の内部には、クライアントＣＰＵ１０４（これはタイムキーピング以外にも多くの機能を実行する）、クライアントＴＯＤクロック１０８、専用鍵レジスタ１１０と公開鍵レジスタ１１２、内部電子記憶装置（キャッシュ）２１２、認証時刻インジケータ２１８、精度持続レジスタ２２０、及び更正調整レジスタ２２２がある。クライアントＣＰＵ１０４はさらに、制御、論理、及び演算回路（図示せず）の他に、暗号化／解読プロセッサ１０６とクロック更正器２２４、及びＣＰＵがセキュア・タイムキーピング装置２１４の他の様々な構成要素の設定と読取りを行うための電子回路を備えている。クライアントＴＯＤクロック１０８は、ＣＰＵ１０４からの時刻と日付の値及びクロック更正器２２４からの更正調整を受信するための入力を備えている。同様に、ＣＰＵ又はプログラムの要求に応じて時刻と日付の値を与えるための出力も備えている。クライアントＴＯＤクロックは、公知の文献による様々ないずれの手法によって実現されるものでもよく、全ての構造部品は物理的に安全確保された電子パッケージ２１６に収納されている。好適例は、クロック・パルス発生器により増分されるクロック・レジスタを含む。

【００２０】動作中に、クライアント・コンピュータ・システム１０２は、入力装置２０６を介して命令を受取り、内部記憶装置２１２及び外部記憶装置２０８に対してデータの読取りと書込みを行い、表示画面２０４上に状態、結果及び他のフィードバックを出力することにより、認証された時刻を用いる又は用いない有用なタスクを処理する。システムのパワーオン時及びシステムがＴＯＤクロック１０８の認証された時刻値なしで動作する他の全ての時点においては、認証時刻インジケータ２１８はＣＰＵ１０４によりＦＡＬＳＥにセットされる。セキュア・タイムと無関係なタスクは、通常どおり実行される。ＴＯＤクロック１０８は、ユーザ、ソフトウェア又は別のシステム等が任意の値にセットしてもよい。しかしながら、認証時刻インジケータ２１８は、物理的に安全確保された電子パッケージ２１６内のＣＰＵ１０４以外のものによってはセットできない。その一方で、認証時刻インジケータ２１８は、コンピュータ・システム１０２内で実行されるいずれのプログラムも読取り専用ベースで利用することができる。従って、もし時間制限のあるライセンスをもつプログラムが開始された場合、又はユーザが時間制限のあるライセンスをもつメディア（録音、映画等）を使用しようとする場合、開始ソフトウェアは、認証時刻インジケータの値を読取ることによりＴＯＤクロック値が実行開始を許可するベースとして信頼できるか否かを速やかに判断することができる。もしその値がＦＡＬＳＥである場合、実行は拒否される。さらに好適例においては、妥当性検証プロセスが損われることを防ぐために、開始ソフトウェア自身が暗号化されたコード・セグメントで実行される。このプロセスについての詳細は前述の米国特許出願第９２８８５０号に記載されている。

【００２１】コンピュータ・システムがＴＯＤクロック１０８の認証された時間で動作しているとき、認証時刻インジケータ２１８はＣＰＵ１０４によりＴＲＵＥにセットされている。セキュア・タイムと無関係なタスクは、尚、通常どおり行われる。もし、もし時間制限のあるライセンスをもつプログラムが開始された場合、又はユーザが時間制限のあるライセンスをもつメディアを使用しようとする場合、開始ソフトウェアは認証時刻インジケータの値を読取り、ＴＯＤクロック１０８が信頼できる時間を有することをＴＲＵＥ応答から検知する。そ

れからＴＯＤクロック１０８内の現在時刻と日付を読取り、実行を許可できるか否かを判断するために許可基準と比較する。表示画面２０４に示すように、システム・ユーザは、認証時刻インジケータの値と同様に、暗号化されていない形の現在時刻と日付に容易にアクセスすることもできる。

【００２２】信頼できるセキュア・タイムによりＴＯＤクロック１０８がセットされた後、精度持続レジスタ２２０、更正調整レジスタ２２２及びクロック更正器２２４が、ＣＰＵ１０４の制御の下に協力することにより、ＴＯＤクロック１０８の現状の精度を維持し、ＴＯＤクロックの精度がもはや信頼できなくなる時点を確定する。更正調整の基本的な目的は、クロックの進みや遅れを補償することである。更正調整レジスタ２２２は、サーバにより与えられる値を格納しており、この値はクロック更正器２２４により用いられて、延長時間の間にその精度を維持するために必要なＴＯＤクロック１０８の値を調整する。好適例では、更正調整レジスタ２２２は、調整間隔と調整極性とを指定する符号をもつ値を格納している。この値はクロック更正器２２４へ与えられ、クロック更正器２２４は、最後の更正調整からのＴＯＤクロックの増分の数が調整間隔に等しくなるまでその増分を監視する。調整間隔は更正調整レジスタ２２２の絶対値である。増分が調整間隔に等しくなったならば、クロック更正器２２４は増分１つ分だけＴＯＤクロック１０８を調整する。この調整の極性は、更正調整レジスタ２２２の極性により決定される。よって、もしこのレジスタ内の値の符号が正であれば、余分の１つの増分により正の調整がＴＯＤクロック１０８に適用される。もしこのレジスタ内の値が０であれば、調整は行われない（増分は０）。一旦更正調整が行われると、クロック更正器はリセットされ、このプロセスが繰返される。

【００２３】精度持続レジスタ２２０は、サーバにより与えられる値を格納しており、この値はＴＯＤクロック１０８がもはや信頼できなくなる時点を示す。この値は認識することにより、ＴＯＤクロック１０８の経時的不安定さの関数として与えられる。つまり、（更正器２２４により修正される）ＴＯＤクロック１０８に関するクロック・ドリフトが変動する、すなわち定期的な更正調整によっては完全に修正することはできないとの認識である。好適例では精度持続レジスタ２２０は日付及び時刻の値を格納している。ＣＰＵ１０４の制御により、この値は定期的にＴＯＤクロック１０８の現在値と比較される。この比較は、時間の加算時点、日付の加算時点、更正調整時、ＴＯＤクロック１０８の読取り時、又は精度持続値を越えないことが十分に保証される他のいずれかの基準時点をきっかけとして実行される。精度持続値に到達したとき、ＣＰＵ１０４は認証時刻インジケータをＦＡＬＳＥにセットしてＴＯＤクロック１０８の時刻

と日付の値がもはや信頼できないことを示す。

【００２４】好適例においては、セキュア・タイムキーピング装置２１４の種々の構成要素へアクセスしようとするクライアント・クロック保守ソフトウェア、許可ソフトウェア、及びクライアント・システム・ユーザが利用するために構築された命令が設けられている。SET CURRENT TIME命令は、クライアントＴＯＤクロック１０８、精度持続レジスタ２２０、及び更正調整レジスタ２２２のために暗号化された値又は暗号化されていない値を受取り、これらの値を対応する場所に格納するように設けられている。SET CURRENT TIME命令については、オペランドが暗号化されている場合に認証時刻インジケータがＴＲＵＥにセットされ、暗号化されていない場合にＦＡＬＳＥにセットされる。サーバのみが専用鍵により暗号化された時刻情報を与えることができるので、ユーザは現在時刻をセットすることはできるが、SET CURRENT TIME命令を呼出して認証時刻インジケータにＴＲＵＥ値をセットすることはできない。

【００２５】セキュア・タイムキーピング装置２１４から値を検索するために、GET CURRENT TIME命令が設けられている。この命令は、暗号化されている（信頼性がある）か暗号化されていないか（信頼性がない）に拘らずいずれのクライアント・ソフトウェアであっても、これを用いてＴＯＤクロック１０８、認証時刻インジケータ２１８、精度持続レジスタ２２０、及び更正調整レジスタ２２２の値を読取ることができる。

【００２６】SET CURRENT TIME命令及びGET CURRENT TIME命令の双方ともマルチプル・アトミック命令として実動化され、それぞれがセキュア・タイムキーピング装置２１４の１つの構成要素をセットし又は検索することを注記する。さらに、暗号化されたデータを処理する際にSET CURRENT TIMEにより実行される機能は、外部で構築された命令を用いることなくセキュア・タイムキーピング装置２１４内で実動化される。すなわち、Ｉ／Ｏポート１１４において暗号化された時刻情報を受取ると、ＣＰＵ１０４は、クライアント・ソフトウェアに誘引されることなくその時刻情報を解読し、それをＴＯＤクロック１０８、精度持続レジスタ２２０、及び更正調整レジスタ２２２に格納する。

【００２７】クライアント・コンピュータ・システム１０２は、セキュア・タイムの要求－受信ネットワークにおいて動作する場合は、定期的にセキュア・タイム伝送を開始しなければならない。あるいは、セキュア・タイムのブロードキャスト（同報通信）・ネットワークにおいて動作する場合は、サーバがクライアントの要求を必要とせずに定期的に伝送を開始する。要求－受信ネットワークにおいては、クライアント・コンピュータ・プロセッサ２０２はサーバ１２０へセキュア・タイム要求を送ることによりセキュア・タイム伝送を開始する。この要求はＣＰＵ１０４により生成され、セキュア・タイム

15

キーピング装置２１４の種々の構成要素の現在値を含む。すなわち、ＴＯＤクロック１０８、認証時刻インジケータ２１８、精度持続レジスタ２２０、更正調整レジスタ２２２、及び公開鍵１１２の値を含む。好適例では、この情報はGET CURRENT TIME命令を用いて簡便に集積され、さらに記録－再生問題を避けるためにＭＡＣを含む。いずれにしてもこの情報は、暗号化／解読プロセッサ１０６により、クライアントの公開鍵とともに伝送に含まれるクライアントの専用鍵を用いて暗号化され、Ｉ／Ｏポート１１４を介してサーバ・システムへ伝送される。引続いて図４に示すように、サーバ・システムは、新しい精度持続値及び新しい更正調整値を計算し、新しいクライアントＴＯＤクロック値を発生し、クライアントの公開鍵に対応する専用鍵を用いて（好適例ではＭＡＣも同様に）この情報を暗号化し、そして暗号化された情報をクライアント・コンピュータ・システム１０２へ返す。この情報を受取ると、暗号化／解読プロセッサ１０６は、専用鍵１１０を用いてこれらの新しいＴＯＤクロック値、精度持続値、及び更正調整値を解読する。好適例では、ＭＡＣもまた解読され、サーバ応答をクライアント要求と照合するために用いられる。その後、ＣＰＵ１０４は、新しいＴＯＤクロック値をＴＯＤクロック１０８に、新しい精度持続値を精度持続レジスタに、そして新しい更正調整値を更正調整レジスタ２２０に格納することによりセキュア・タイムキーピング装置２１４の他の種々の構成要素を設定する。最後に、暗号化された時刻及び日付の値が無事に処理され、認証された信頼できるＴＯＤクロック値が現在用いられていることを示すべく認証時刻インジケータ２１８がＴＲＵＥにセットされる。

【００２８】セキュア・タイムのブロードキャスト・ネットワークにおいては、クライアント要求が発生しない点を除けばクライアントの動作は上記と同様である。そのかわりにサーバは、クライアント専用鍵により暗号化されクライアント公開鍵に対応させることにより識別されるセキュア・タイム・ブロードキャストを定期的に発生する。あるいは、全てのクライアントに暗号化されたマスタ鍵を送信した後に１つのセキュア・タイム・ブロードキャストを全てのクライアントに同時に送り、そしてこのブロードキャストは先に送られた時刻マスタ鍵を用いてクライアントにおいて解読される。これらのブロードキャストは要求されたものではないので、サーバは新しい精度持続値及び更正調整値を作成するために十分なデータをもっていない。つまり、このモードの動作には、それらの情報が包含されない。ブロードキャストのセキュア・タイム伝送を受取ると、上記のように新しいＴＯＤクロック値が解読されてＴＯＤクロック１０８へ与えられ、認証時刻インジケータ２１８がＴＲＵＥにセットされる。

【００２９】好適例においては、メッセージの確認が必

16

要な場合、クライアントが最初のＭＡＣを含む伝送を予め行うことによりブロードキャスト・モードを開始する。それに続いてサーバがセキュア・タイム伝送をクライアントへブロードキャストするとき、これに最初のＭＡＣを含める。クライアントは、サーバが次のセキュア・タイム伝送を行うときに用いるための新しいＭＡＣを送ることにより受信を確認する。その後の各ブロードキャストにおいてこのプロセスが繰返される。さらに、このＭＡＣを伴うブロードキャスト・モードの動作において、クライアントの確認の中にクライアントＴＯＤクロック、認証時刻インジケータ、精度持続レジスタ、及び更正調整レジスタの値を含めてもよい。それによって、ブロードキャスト・モードにおける上記の欠点をある程度改善し、サーバがその次のブロードキャストで更新された精度持続値及び更正調整値を与えることが可能になる。これらの値は要求－受信モードにおけるものと比べると正確ではないであろう。なぜなら、次のブロードキャストはそれらの値のベースとされた確認よりもずっと後に行われるものだからである。しかしながら、この問題自体は、クライアントのバンド幅制限内でブロードキャスト頻度を増すことにより対処できるであろう。

【００３０】図３は、クライアント・コンピュータ・システム１０２における電源の保全性を監視するために設けられた付加的な機構である。電源保全モニタ３０２は、物理的に安全確保されたパッケージ２１６内のセキュア・タイムキーピング装置２１４に付加される。電源保全モニタ３０２は、モニタ用電子回路（破線で示す）を介して、ＣＰＵ１０４、ＴＯＤクロック１０８、認証時刻インジケータ２１８、精度持続レジスタ２２０、及び更正調整レジスタ２２２を含むセキュア・タイムキーピングの他の構成要素に接続される。動作中、電源保全モニタ３０２は、クライアント・コンピュータ・システムで使用される電子素子の作動限界に相当する予め設定された正常範囲に対して継続的に上記の構成要素の電圧レベルを監視する。もし、供給される通常の電圧又はバックアップ用の電圧が、セキュア・タイムキーピング装置の構成要素の安定した正確な動作を維持する範囲外に低下したならば、電源保全モニタ３０２は認証時刻インジケータ２１８の値をＦＡＬＳＥにセットし、ＴＯＤクロック１０８がもはや信頼できないことを示す。

【００３１】電源保全モニタ３０２については多くの変型が可能である点を注記する。例えば、セキュア・タイムキーピング装置の全ての構成要素を監視するのではなく、電源保全モニタ３０２がＴＯＤクロック１０８の電圧のみを監視する、又は他の構成要素のいずれかのみを監視するように構成してもよい。別の例として、セキュア・タイムキーピング装置２１４への電源経路を、単一の電源入力パスを設けるように設計してもよい。この場合、電源保全モニタ３０２は個々の構成要素を監視するのではなくその電源入力パスを直接監視すればよい。最

17

終的には、３０２内で電源保全監視機能を行うべく選択された特定の電子素子及び低レベル素子が、設計選択の根拠となる。これについては公知の多くの文献があるので、ここでは繰返さない。

【００３２】図４は、本発明によりクライアント・コンピュータ・システムへセキュア・タイム伝送を行うサーバ・コンピュータ・システムの構造と作用を詳細に示した機能図である。サーバ・コンピュータ・システム（セキュア・タイム・サーバ）１２０は、物理的に安全確保されたデータ・センタに設置されている。システム１２０は、サーバＣＰＵ１２２、サーバＴＯＤクロック１２６、Ｉ／Ｏポート１２８、公開鍵及び専用鍵の記憶領域１３０、並びに更正／安定度履歴の記憶領域４０２を含む。サーバＣＰＵ１２２自身は、暗号化／解読プロセッサ１２４、安定度監視プロセッサ４０４、及び更正プロセッサ４０６を含む（もちろん、通常ＣＰＵが行う多くの機能のための構成要素も含む）。ＴＯＤクロック１２６は、時刻クロックと日付カレンダーを備える。これらは、非常に正確な時間ソースに基づいていることが好ましく、協定世界時、グリニッジ標準時、又はいずれかの地域時にセットされていればよい。Ｉ／Ｏポート１２８は、電子通信ネットワークを介して１又は複数のクライアント・コンピュータ・システムへ接続され、クライアントＴＯＤクロック値をクライアントの更正及び安定データとともに受取りかつ新しいクライアントＴＯＤクロック値を新しい更正及び安定データとともにセキュア・タイム要求者へ送るためのＩ／Ｏ機構を提供する。鍵記憶領域１３０及び更正／安定度履歴記憶領域４０２は、ＲＡＭ、ディスク、テープ等の任意のデジタル記憶媒体に保持される。

【００３３】要求－受信モードの動作においては、Ｉ／Ｏポート１２８を介してセキュア・タイム要求が受信されたときにサーバ動作が開始される。先ず、サーバ暗号化／解読プロセッサ１２４により要求が解読される。解読に続いて、受信した認証時刻インジケータの値が調べられる。もしこれがＦＡＬＳＥであれば、クライアント要求の中の他の情報は無視される。現在時刻及び日付がＴＯＤクロック１２６から得られ、クライアントの更正調整値及び精度持続値の履歴が更正／安定度履歴記憶領域４０２から得られ（あるいは、そうしない場合は更正調整値及び精度持続値としてデフォールト値が選択される）、全ての情報が暗号化／解読プロセッサ１２４による暗号化され、そして暗号化されたデータが、Ｉ／Ｏポート１２８を介して要求を行っているクライアントへ伝送される。

【００３４】もし、受信された認証時刻インジケータがＴＲＵＥであれば、クライアントのＴＯＤクロックがセキュア・タイムを用いてセットされ且つ今尚信頼できることを示している。従って、次にサーバ・システム１２０は、受信したクライアントＴＯＤクロック値、精度持

18

続値、及び更正調整値を用いて新しい精度持続値及び更正調整値を発生する。特に、新しい更正調整値を発生するために、更正調整プロセッサ４０６は、ＴＯＤクロック１２６の現在の値と受信されたクライアントＴＯＤクロック値とを比較し、それによってクライアントの更正調整値を修正する。好適例では、前の値の効果を評価しその情報をフィードバックして最適値に徐々に近づけて行くことにより新しい更正調整値を決定するような試行錯誤的手法が用いられている。この手法の特定の実施例においては、ＴＯＤクロック１２６の現在値と受信されたクライアントＴＯＤクロック値との差を、クライアントＴＯＤクロックがセットされてからこれに対して行われた更正調整の全数と足し合わせ、そしてその結果を、クライアントＴＯＤクロックが新しい更正調整値を決定するためにセットされてからの期間における増分の全数で割る。この値は、次にこのクライアントからのセキュア・タイム要求を受信したときに利用できるよう安定度履歴記憶領域４０２へ記憶される。

【００３５】新しい精度持続値を発生するために、クライアントＴＯＤクロックがセットされてからの期間にクライアントＴＯＤクロック値に積算されたエラー（先に更正調整値に関連して決定されている）が、安定度監視プロセッサ４０４により、クライアントＴＯＤクロックの許容できる不安定さを時間の関数として定めた予め設定された基準と比較される。新しい精度持続値は、先の不安定レベルが、精度持続する全体に亘ってクロック・エラーの許容量よりも大きくならないように選ばれる。この値は、次にこのクライアントからのセキュア・タイム要求を受信したときに利用できるよう安定度披瀝記憶領域４０２に記憶される。更正調整値のときと同様に、好適例では、前の値の効果を評価しその情報をフィードバックして最適値に徐々に近づけて行くことにより新しい更正調整値を決定するような試行錯誤的手法が用いられている。

【００３６】精度持続情報及び更正調整情報の履歴を保持することに関しては、多くの変型が可能であることを注記する。例えば、精度持続レジスタ及び更正調整レジスタの十分な履歴値を、サーバ履歴記憶領域４０２内に保持することにより、これらの項目をクライアント要求から省くことができる。あるいは、精度持続値についての全履歴情報を保持するが更正調整値については全く保持しなくてもよい。又はそれと逆に、クライアントに対してそのセキュア・タイム要求の中で保持していたのではない値を送るよう要求する。

【００３７】上記の新しい精度持続値及び更正調整値を発生の後、サーバＴＯＤクロック１２６の現在値とともに双方の値が、暗号化／解読プロセッサ１２４により要求しているクライアントに対応する専用鍵を用いて暗号化される。暗号化されたデータは、Ｉ／Ｏポート１２８を介して要求しているクライアントへ伝送される。

19

【００３８】サーバ・コンピュータ・システム１２０がブロードキャスト・モードで動作している場合、前述のように、新しい精度持続値及び更正調整値を発生するために必要な情報をサーバ・コンピュータ・システム１２０が得ることができない。この場合、安全確保されたＴＯＤクロック値のみがブロードキャストされる。別の例として、精度持続値及び更正調整値の履歴を安定度履歴記憶領域４０２から得てもよく、あるいはデフォールト値を発生して暗号化しＴＯＤクロック値とともにブロードキャストしてもよい。さらに別の例として、ブロードキャスト・モードを要求－受信モードの間に適宜挿入することにより、ある選択期間には時刻のみを更新し、別の選択期間にはセキュア・タイム装置の更新を行うようにしてもよい。又は、ＭＡＣを伴うブロードキャスト手法を用いることにより、クライアント確認が少なくともクライアントＴＯＤクロック値を含むようにしてもよい。

【００３９】まとめとして、本発明の構成に関して以下の事項を開示する。

【００４０】（１）物理的に安全確保されたパッケージ内に設置された中央演算処理装置と電子記憶装置とを含むコンピュータ・システムにおいて用いるセキュア（安全確保された）・タイムキーピング装置であって、時刻伝送及び日付伝送を暗号化しかつ解読するために専用鍵を識別するときに用いる公開鍵を保有する公開鍵レジスタと、前記専用鍵を保有する専用鍵レジスタと、前記専用鍵を用いて暗号化された時刻及び日付の情報を受信する入力と、前記専用鍵を用いて受信された時刻及び日付の情報を解読するデータ解読手段と、前記解読された時刻及び日付の情報を受信するための入力及び暗号化されていない時刻及び日付の情報を与えるための出力を備え、時刻クロックと日付カレンダーとを含む日時（time-of-day：ＴＯＤ）クロックとを有するセキュア・タイムキーピング装置。

（２）前記ＴＯＤクロックが前記中央演算処理装置と同じ物理的に安全確保されたパッケージ内に設置される上記（１）に記載のセキュア・タイムキーピング装置。

（３）前記公開鍵が、前記コンピュータ・システムのシステム・シリアル番号に対応する上記（１）に記載のセキュア・タイムキーピング装置。

（４）前記公開鍵が前記コンピュータ・システムに固有のものでありかつ物理的に安全確保されたパッケージの外部からアクセス可能である上記（１）に記載のセキュア・タイムキーピング装置。

（５）前記専用鍵が前記コンピュータ・システムに固有のものでありかつ物理的に安全確保されたパッケージの外部からアクセス不能である上記（１）に記載のセキュア・タイムキーピング装置。

（６）前記専用鍵を用いて暗号化された現在の時刻及び日付の情報のいずれかを時刻サーバに対して要求するセキュア・タイム（安全確保された時刻）要求手段を有する上記（１）に記載のセキュア・タイムキーピング装置。

20

（７）前記セキュア・タイム要求手段により開始された要求が前記ＴＯＤクロックの現在値を含む上記（６）に記載のセキュア・タイムキーピング装置。

（８）時刻及び日付のいずれかの更正値を受信しかつ該更正値を前記ＴＯＤクロックに適用するクライアント・クロック更正手段を有する上記（１）に記載のセキュア・タイムキーピング装置。

（９）前記更正値が専用鍵を用いて暗号化される上記（８）に記載のセキュア・タイムキーピング装置。

（１０）物理的に安全確保されたパッケージ内に設置された中央演算処理装置と電子記憶装置とを含むコンピュータ・システムにおいて用いるセキュア（安全確保された）・タイムキーピング装置であって、時刻クロックと日付カレンダーとを含む日時（time-of-day：ＴＯＤ）クロックと、前記ＴＯＤクロックが認証された時刻及び日付を有するか否かを示す値を記憶する認証時刻インジケータと、前記ＴＯＤクロックが正確であると見なされる持続時間を示す値を記憶する精度持続レジスタと、時刻、日付、及び精度持続時間のいずれかの値を受信する入力と、前記ＴＯＤクロックからの暗号化されていない時刻及び日付の値と前記認証時刻インジケータからの値を与える出力とを有するセキュア・タイムキーピング装置。

（１１）前記精度持続レジスタが時刻の値を格納し、前記認証時刻インジケータが、暗号化された値を用いて前記ＴＯＤクロックをセットしたことと、暗号化された値を用いて前記精度持続レジスタをセットしたことと、該精度持続レジスタが該ＴＯＤクロックの値より時間的に大きい（遅い）値を格納していることとを満たすことに応答してＴＲＵＥにセットされる上記（１０）に記載のセキュア・タイムキーピング装置。

（１２）前記認証時刻インジケータが、システムの初期化、動作電圧低下状態、ＴＯＤクロックを暗号化されていない値を用いてセットしたこと、及び前記精度持続レジスタが該ＴＯＤクロックの値よりも時間的に小さい（早い）値を格納していることのいずれかに対してＦＡＬＳＥにセットされる上記（１１）に記載のセキュア・タイムキーピング装置。

（１３）受信された時刻、日付、及び精度持続の値に基づいてＴＯＤクロックの値及び精度持続レジスタの値をセットし、受信された時刻、日付、及び精度持続の値が暗号化されていない場合に前記認証時刻インジケータをＦＡＬＳＥにセットし、受信された時刻、日付、及び精度持続の値が暗号化されておりかつ前記精度持続レジスタにセットされた値が前記ＴＯＤクロックにセットされた値よりも時間的に大きい場合に該認証時刻インジケータをＴＲＵＥにセットする時刻装置設定手段を有する上

記（１０）に記載のセキュア・タイムキーピング装置。

（１４）前記セキュア・タイムキーピング装置が、ＴＯＤクロックが更正調整を受信すべき時間間隔を示す値を記憶する更正調整レジスタを有し、前記入力が、更正調整の値を受信するための手段を有し、前記時刻設定手段が、前記受信された更正調整の値に基づいて前記更正調整レジスタをセットする手段を有する上記（１３）に記載のセキュア・タイムキーピング装置。

（１５）操作により前記ＴＯＤクロック及び前記更正調整レジスタに接続されかつ該ＴＯＤクロックが該更正調整レジスタの値に増分される毎に該ＴＯＤクロックに対する更正調整を行うＴＯＤクロック更正器を有する上記（１４）に記載のセキュア・タイムキーピング装置。

（１６）前記更正調整レジスタの値が、増分、飛び、及び非調整のいずれかを示し、更正調整の値が増分を示す場合は、前記ＴＯＤクロックに適用される更正調整が１つの加算的増分であり、更正調整の値が飛びを示す場合は、前記ＴＯＤクロックに適用される更正調整が１つの飛びであり、更正調整の値が非調整を示す場合は、前記ＴＯＤクロックに適用される更正調整が増分ゼロである上記（１５）に記載のセキュア・タイムキーピング装置。

（１７）正の更正調整値が増分を示し、負の更正調整値が飛びを示し、及びゼロの更正調整値が非調整を示す上記（１６）に記載のタイム・キーピング装置。

（１８）前記ＴＯＤクロック、前記認証時刻インジケータ、前記精度持続レジスタ、及び前記更正調整レジスタの暗号化されていない値を読取る時刻装置読取り手段を有する上記（１６）に記載のセキュア・タイムキーピング装置。

（１９）前記更正調整レジスタの値が前記ＴＯＤクロックを最後にセットしてから該ＴＯＤ内に積算されたドリフト量の関数であり、前記精度持続レジスタの値が該ドリフト量と該ＴＯＤクロックの先の設定に対応する予め測定されたドリフト量との比較に基づく上記（１８）に記載のセキュア・タイムキーピング装置。

（２０）現在時刻、日付、及び精度持続の値のいずれかを時刻サーバから要求するセキュア・タイム要求手段を有し、前記セキュア・タイム要求手段により開始された要求が、前記ＴＯＤクロックの現在値、前記精度持続レジスタの現在値、前記更正調整レジスタの現在値、及び認証時刻インジケータの現在値のいずれかを含む上記（１３）に記載のセキュア・タイムキーピング装置。

（２１）時刻クロックと日付カレンダーを含むサーバ日時（time-of-day：ＴＯＤ）クロックを有するコンピュータ・ネットワークにおけるセキュア（安全確保された）・タイム・サーバであって、公開鍵を含むセキュア・タイム要求を受信する入力と、前記公開鍵に対応する専用鍵を識別するプロセッサ手段と、前記専用鍵を用いて前記ＴＯＤクロックからの時刻及び日付の情報を暗号

化するデータ暗号化手段と、前記セキュア・タイム要求を行った者に対して前記暗号化された時刻及び日付の情報を送る出力とを有するセキュア・タイム・サーバ。

（２２）前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び更正履歴の情報、並びに前回のクライアント・クロック更正計算から積算された更正履歴のいずれかに基づいて該クライアント・クロック更正値を計算する更正調整手段を有する上記（２１）に記載のセキュア・タイム・サーバ。

（２３）前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び安定度履歴の情報、並びに前回のクライアント・クロックの安定度計算から積算された安定度履歴のいずれかに基づいて該クライアント・クロックの安定度値を計算するクライアント安定度監視手段を有する上記（２１）に記載のセキュア・タイム・サーバ。

（２４）前記クライアント・クロック更正値が、さらに、前記クライアント・クロックの最後の設定以降該クライアント・クロックに積算されたドリフト量から計算される上記（２２）に記載のセキュア・タイム・サーバ。

（２５）前記更正値が、前記専用鍵を用いて暗号化される上記（２２）に記載のセキュア・タイム・サーバ

（２６）時刻クロックと日付カレンダーを含むサーバ日時（time-of-day：ＴＯＤ）クロックを有するコンピュータ・ネットワークにおけるセキュア（安全確保された）・タイム・サーバであって、セキュア・タイム伝送を行うために公開鍵及び専用鍵を識別するプロセッサ手段と、前記専用鍵を用いて前記ＴＯＤクロックからの時刻及び日付の情報を暗号化するデータ暗号化手段と、前記暗号化された時刻及び日付の情報をブロードキャスト（同報通信）する出力とを有するセキュア・タイム・サーバ。

（２７）前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び更正履歴の情報、並びに前回のクライアント・クロック更正計算から積算された更正履歴のいずれかに基づいて該クライアント・クロック更正値を計算する更正調整手段を有する上記（２６）に記載のセキュア・タイム・サーバ。

（２８）前記サーバＴＯＤクロックの値、クライアントから受信された時刻、日付及び安定度履歴の情報、並びに前回のクライアント・クロックの安定度計算から積算された安定度履歴のいずれかに基づいて該クライアント・クロックの安定度値を計算するクライアント安定度監視手段を有する上記（２６）に記載のセキュア・タイム・サーバ。

（２９）前記クライアント・クロック更正値が、さらに、前記クライアント・クロックの最後の設定以降該クライアント・クロックに積算されたドリフト量から計算される上記（２７）に記載のセキュア・タイム・サー

23

バ。

【００４１】

【発明の効果】本発明によれば、クライアントのＴＯＤクロックをセットするためにサーバが発生した信頼できる時刻値を提供することにより、クライアント・システムは信頼できる時刻値がなくても機能し、さらに一旦信頼できる時刻値を与えると、クライアント・クロックの正確さを維持するような装置が提供される。

【図面の簡単な説明】

【図１】本発明によるセキュア・タイム・クライアント／サーバ・システムを示す機能図である。

【図２】本発明によるセキュア・タイムキーピング装置を含むクライアント・コンピュータシステムを示す機能図である。

【図３】本発明によるクライアント・コンピュータ・システムにおいて用いる電源保全モニタを示す機能図である。

【図４】本発明によるセキュア・タイム・サーバ・システムを示す機能図である。

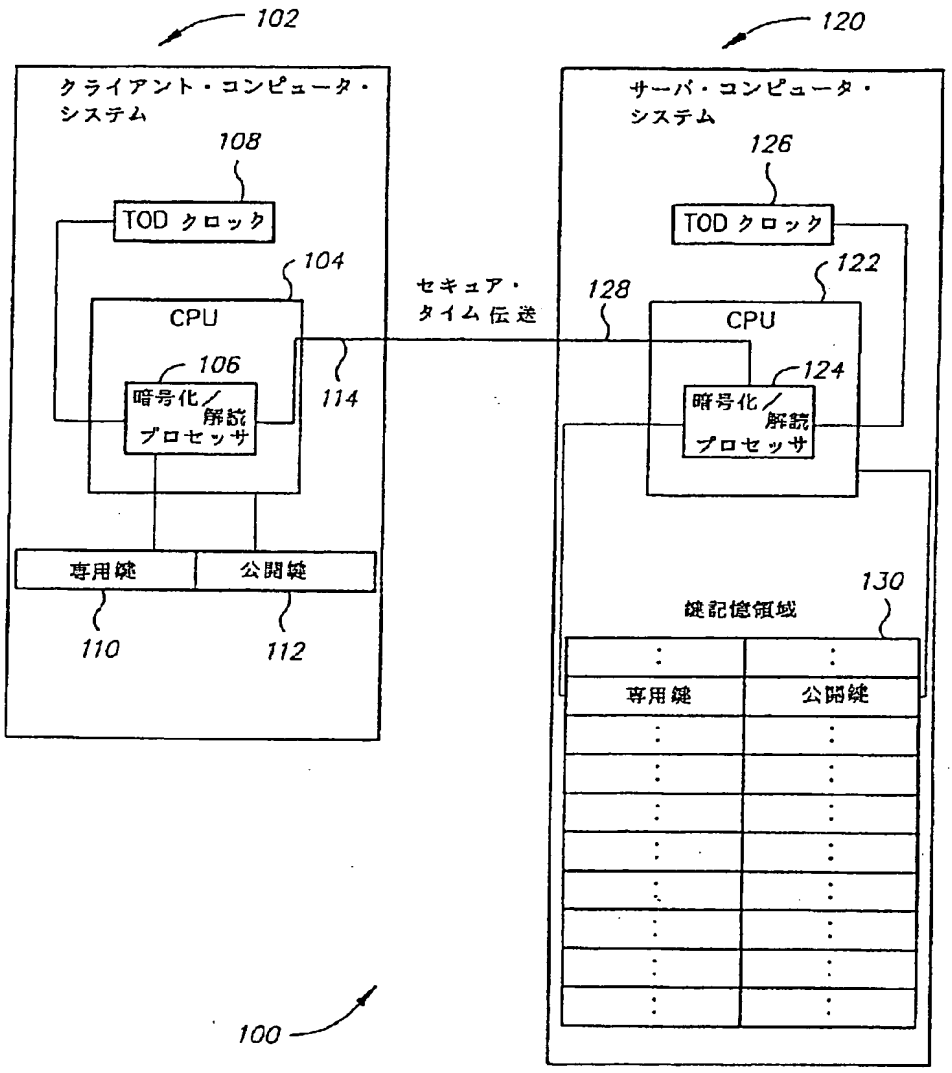
【符号の説明】

１００　セキュア・タイム・クライアント／サーバ・システム

24

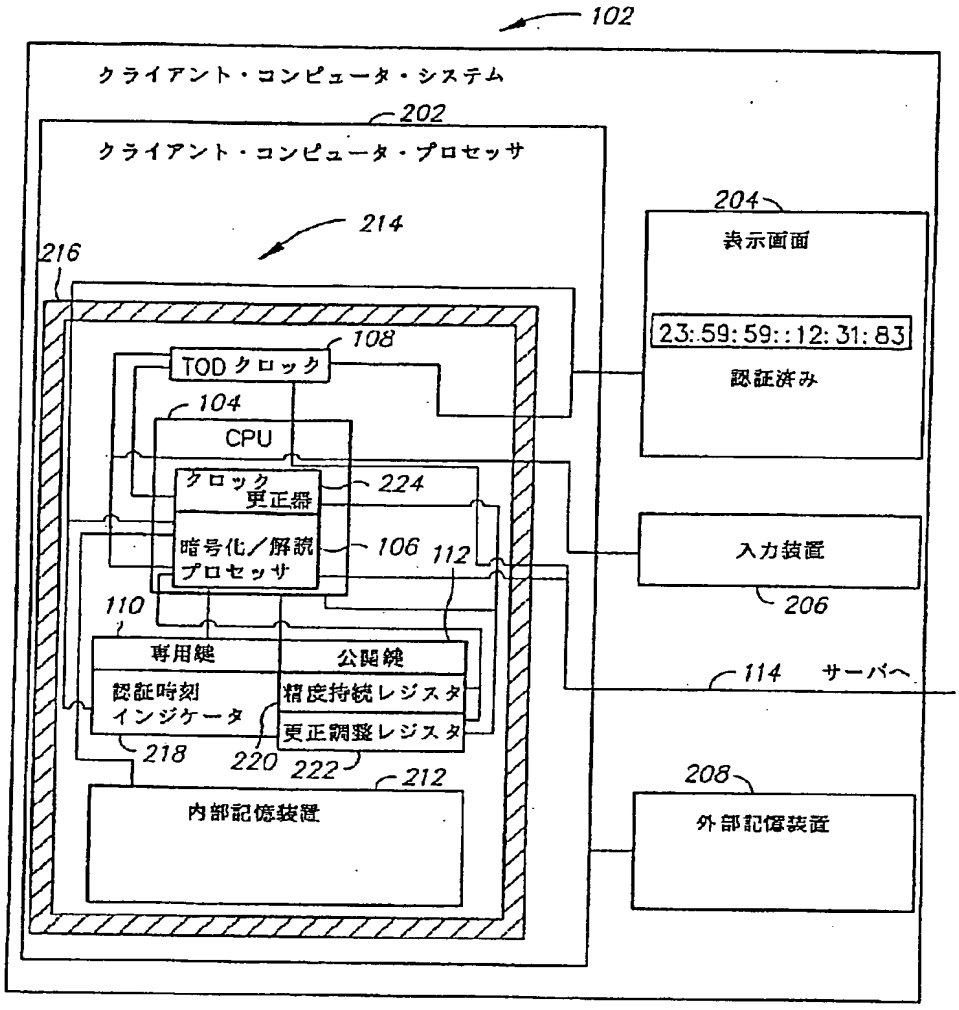
１０２　クライアント・コンピュータ・システム
１０４　クライアントＣＰＵ
１０６　暗号化／解読プロセッサ
１０８　クライアントＴＯＤクロック
１１０　専用鍵
１１２　公開鍵
１２０　サーバ・コンピュータ・システム
１２２　サーバＣＰＵ
１２４　暗号化／解読プロセッサ
１２６　サーバＴＯＤクロック
１３０　鍵記憶領域
２１４　セキュア・タイムキーピング装置
２１６　パッケージ
２１８　認証時刻インジケータ
２２０　精度持続レジスタ
２２２　更正調整レジスタ
２２４　クロック更正器
３０２　電源保全モニタ
４０２　更正／安定度履歴記憶領域
４０４　安定度監視プロセッサ
４０６　更正プロセッサ

【図１】



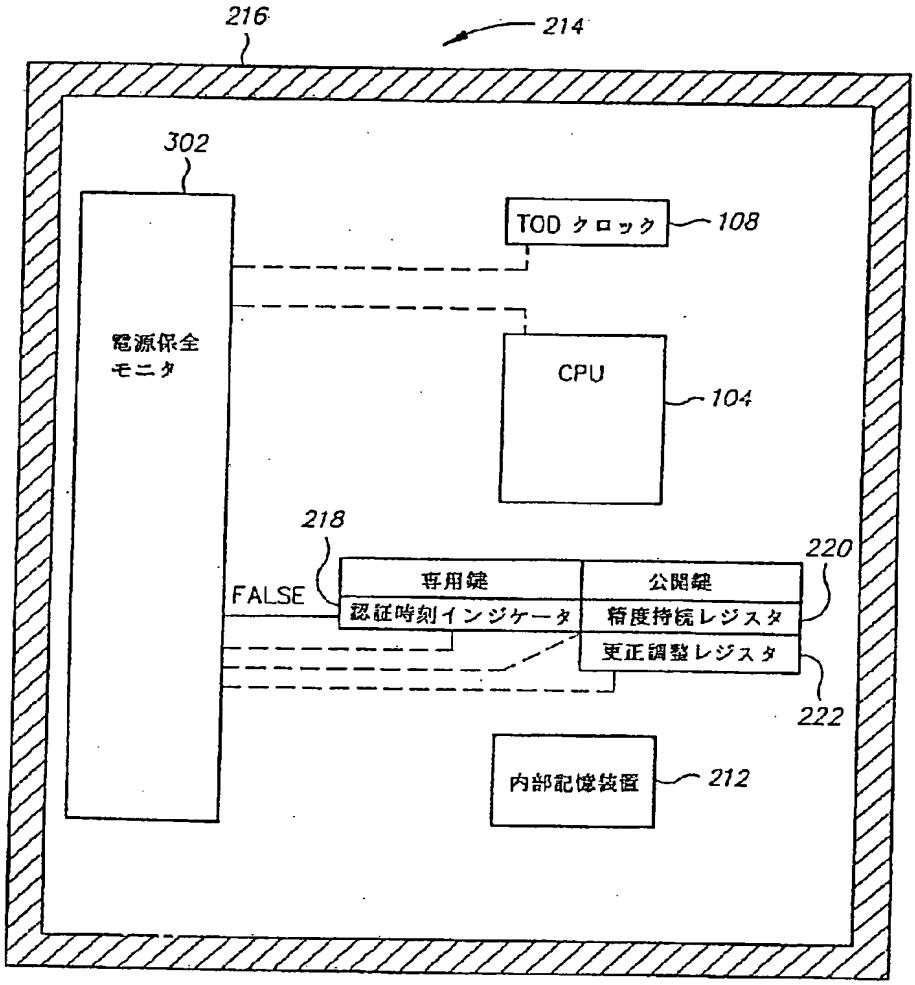
セキュア・タイム・クライアント／サーバ・システム

【図２】



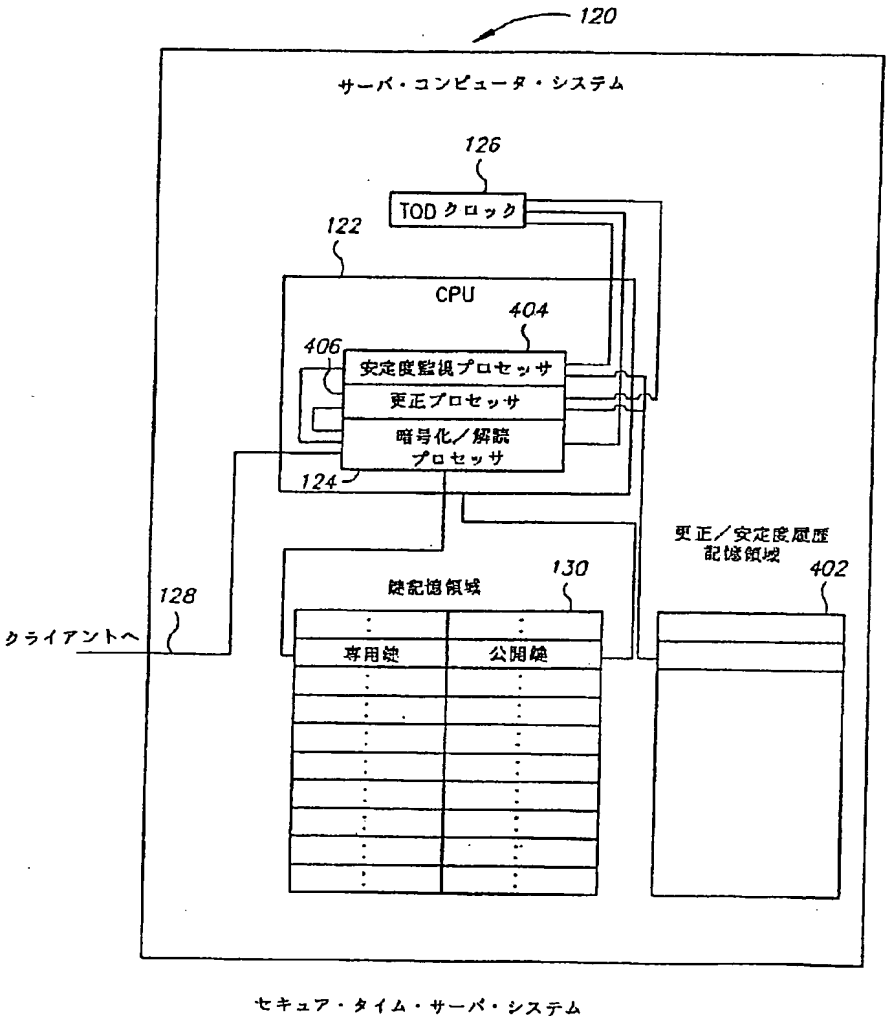
セキュア・タイムキーピング装置を有する
クライアント・システム

【図３】


216
214
302
TOD クロック
108
電源保全
モニタ
CPU
104
218
220
FALSE
専用鍵
公開鍵
認証時刻インジケータ
精度持続レジスタ
更正調整レジスタ
222
内部記憶装置
212

電源保全モニタ

【図４】



セキュア・タイム・サーバ・システム